BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matters of:	)	
	)	
The Cybersecurity Roadmap	)	PS Docket No. 10-146
	)	
	)	
A National Broadband Plan for Our Future	)	GN Docket No. 09-51
	)	
	)	

COMMENTS OF
SAN DIEGO GAS & ELECTRIC COMPANY
REGARDING THE NATIONAL CYBERSECURITY ROADMAP

San Diego Gas & Electric Company ("SDG&E") submits its comments in response to the Commission's Public Notice regarding the development of a national cybersecurity roadmap. By the Public Notice, the Commission requested comments related to, among other things, its investigation of the vulnerabilities in the communications network with respect to, and the development of countermeasures and solutions in preparation for and response to, cyber threats and attacks.[1] SDG&E fully agrees with the Commission that these matters are of the utmost importance and that the urgency of addressing the potential threats to the national economy and security is increasing. SDG&E's utilization of the national broadband communications network as part of its own smart electricity grid ("the smart grid") is, in some measure, dependent upon the reliability and security of the national communications network. The smart grid represents critical infrastructure in its own right and its constituent components, including those broadband facilities and services being incorporated into the energy industry's communications network, must contribute to, or at the very least maintain, the level of reliability and security of the national energy-delivery system. SDG&E expects the Commission's cybersecurity roadmap will provide the additional and reasonable assurances these ends can and will be achieved.

[1] See Public Notice, *Comment Sought on National Broadband Plan Recommendation to Create a Cybersecurity Roadmap,* DA 10-1354 (released August 9, 2010).

A. Introduction

SDG&E is a regulated public-utility gas and electric corporation operating pursuant to authorities granted by the Federal Energy Regulatory Commission and the California Public Utilities Commission. The company provides integrated gas and electric services to over one million customers in San Diego and Orange Counties, California. SDG&E is among the companies leading the utility industry in the development and deployment of operational and customer-service strategies enabled by smart-grid technologies, applications and functionalities. As part of the National Broadband Plan, the Commission echoed the sentiments of Congress by recognizing the importance of the smart grid to the growth of the national economy and environment.[2] SDG&E's current smart-grid plans and activities fully comport with the Commission's expectations that vital elements of the electricity infrastructure will in part rely upon broadband communications to facilitate their deployment and efficient operation.[3]

As the Commission recognized in the National Broadband Plan, protecting the national broadband network and its users from cyber attacks and security breaches is a critical aspect of the engineering and operation of the network. SDG&E provides the following comments regarding the manner in which cybersecurity issues should be addressed in the context of the development, implementation and operation of the emerging smart electricity grid.

B. Comments of SDG&E on the Cybersecurity Roadmap

1. Identification of Threats

SDG&E believes the cybersecurity risks posing the greatest concerns to the energy industry are well described in the National Broadband Plan. SDG&E has previously provided comments to the Commission noting that it expects to use a combination of private and carrier-provided broadband services to link certain utility assets and locations for the purposes of system monitoring, control and management. The relative and eventual mix of public and private services will ultimately be determined by the comparative costs of the available options and the suitability of those options to SDG&E's specific operational needs. This evaluation will include an assessment of the adequacy and effectiveness of the cybersecurity measures taken by public

[2] See Omnibus Broadband Initiative, Federal Communications Commission, *Connecting America: The National Broadband Plan,* (March 2010), at Chapter 12. "Energy and the Environment", at p.245.

[3] SDG&E previously provided the Commission with details related to its smart-grid program in the Comments filed by the Sempra Energy Utilities in this docket on October 2, 2009.

carriers to harden and secure their facilities and the ability of those carriers to recover from adverse events.

As the Commission has noted time and again, the cybersecurity roadmap must address intentional, criminally motivated attacks on the national broadband system – the importance of this aspect of the cybersecurity roadmap cannot be overstated where such attacks are aimed at and could potentially result in the disruption of the vital services and products provided by the nation's electricity industry. Among the most important hallmarks of the domestic power industry is its exceptional record of reliability. Thus, SDG&E's election to use a carrier-provided network would be predicated upon an assumption that those networks are virtually invulnerable to attacks aimed at (a) intercepting, corrupting, stealing, altering, or destroying data being transmitted by the utility or (b) manipulating control systems that manage the electricity grid and ancillary systems. Because SDG&E recognizes that the combination of determination and sophistication can thwart even the best, state-of-the-art security measures, SDG&E agrees with the Commission that special attention should be given in the cybersecurity roadmap to taking appropriate steps to assure rapid service recovery following natural or perpetrated disasters and outages affecting the national communications system.

2. Detection, Notification and Remediation of Threats: Federal Roles

SDG&E fully supports the design and implementation of the federal response to cyber threats and attacks embodied in the National Infrastructure Protection Plan.[4] The Plan responds to Homeland Security Presidential Directive No. 7[5], charging federal agencies with the responsibility to identify and prioritize critical infrastructure and key resources, and protecting them from attack. Under the Plan, the Commission is among several federal agencies responsible for the Sector-Specific Plan for the Communications Sector. SDG&E anticipates that the development of the cybersecurity roadmap as described in the National Broadband Plan and in the Public Notice will continue the Commission's contributions to and coordination with these prior federal efforts.

---

[4] See the *2009 National Infrastructure Protection Plan*, available at the following web address: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[5] See *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection,* December 17, 2003, available at the following web address: http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.

For its part, the Commission should be commended for the role it plays in detecting, abating and responding to cyber threats to the critical infrastructure and key resources in the communications sector. The national carrier network is, quite plainly, near-ubiquitous in scope and operation. Unfortunately, this allows attacks on a local electric system to be launched from remote and even foreign locations. This makes it far from SDG&E's own capabilities to detect or address threats posed by rogue access points which can be located anywhere, are highly mobile and transitory, and can be used to intercept and corrupt data transmissions or generate and propagate illegitimate data. With only limited resources and reach, neither SDG&E nor local authorities can effectively combat threats posed by distant and foreign attackers. The Commission and its partner federal agencies have these larger capabilities, augmented by the ability of the federal government to negotiate, implement and manage international partnerships addressing cyber threats from abroad. In terms of the roles specific federal agencies might play in addressing threats to cybersecurity at the intersection of the energy and communications sector, and specifically as to the multi-sector interdependencies that exist in the smart electricity grid, SDG&E believes it would be useful to distinguish between two separate jurisdictional functions.

The first function is related to system design and engineering standards. As the Commission is aware, the Federal Energy Regulatory Commission ("the FERC") has been charged by Congress with the development of interoperability standards for smart-grid equipment, software, applications, and functionalities.[6] The FERC has already launched a rulemaking that will result in the setting of smart-grid interoperability standards within the foreseeable future. To accomplish its objectives, the FERC has enlisted the considerable expertise and experience of the National Institute of Science and Technology in this effort.[7] In addition, the FERC has already adopted standards and regulations related to the protection of critical infrastructure, a portion of which address cybersecurity. The management and enforcement of these standards and regulations has been delegated to the National Electricity Reliability Corporation and its various regional subdelegates.[8] Finally, the Department of

[6] See *Energy Independence and Security Act of 2007,* Public Law No. 110-140, 121 Stat. 1492 (2007).
[7] See *Re Smart Grid Policy,* Federal Energy Regulatory Commission Docket No. PL09-4-000, 128 FERC ¶61,060.
[8] See Critical Infrastructure Protection (Cyber Security Standards), Nos. CIP-001-1, *et seq*., available at http://www.nerc.com/page.php?cid=2|20. With respect to these standards and regulations, SDG&E is subject to the oversight of the Western Electricity Coordinating Council, the FERC subdelegate with jurisdiction over electric

Energy has adopted its own rules and regulations related to cybersecurity. These rules and regulations are applied to federal contractors providing electricity services and facilities to the federal government; as an example, SDG&E is subject to the Department's cybersecurity regulations in the context of the Department's grant of funds to SDG&E, awarded under the aegis of the American Recovery and Reinvestment Act of 2009, that will be used to finance certain aspects of the deployment of SDG&E's smart grid.[9]

Given the previous and expert attention that has been given to standards and regulations related to the technical specifications and interoperability of the various elements of the smart electricity grid, the Commission may rely upon the existing federal regulatory apparatus in the energy sector to develop, apply and formulate appropriate engineering and design regulations in these areas. The Commission should take cognizance of those regulations and standards and consult with the appropriate agencies as it determines the manner in which the national broadband policy and national broadband architecture can facilitate the rapid deployment of smart-grid technologies and equipment.[10] This should be orchestrated so that the Commission's engineering and design standards and regulations governing communications equipment and networks are harmonized with existing smart-grid regulations and standards and, ultimately, contribute to security objectives and regulations. A collaborative interagency system of engineering and design rules is necessary and appears to be workable for these matters, assuring that the jurisdictions and domain expertise of concerned agencies are all taken into consideration.

The second regulatory function concerns matters more related to the policing of the national communications system to assure that cyber threats are detected, isolated, mitigated, abated or defeated, and punished. From SDG&E's perspective, the National Infrastructure Protection Plan provides for the appropriate blend of, on the one hand, oversight and coordination of federal efforts by a primary agency and, on the other hand, the appropriate delegation of responsibilities to specific agencies where sector or local expertise exists and should be brought to bear. This lays the foundation for cooperation between the many interested federal agencies that can and should contribute to a comprehensive, integrated national effort,

---

utilities operating in the Western Interconnection that encompasses all or a portion of fourteen states and certain facilities comprising the interconnected electricity systems of southwestern Canada and northwestern Mexico.

[9] See *American Recovery and Reinvestment Act of 2009*, Public Law No. 111-5, 123 Stat. 115 (2009).

[10] The Commission has previously acknowledged the importance of the adjacent jurisdictions relevant to energy-regulated cybersecurity regulations. See *Connecting America: The National Broadband Plan, supra,* at pp. 252, 253, (Recommendations 12.3 and 12.6).

but importantly assures that a primary agency takes responsibility for bringing all of these efforts together within the overarching mission and shared purpose of protecting the nation's critical infrastructure and key resources. In SDG&E's experience, this organizational design has enabled the effective collection, interpretation and sharing of vital national and international intelligence regarding potential and preventive measures, with the active involvement of both federal and local law enforcement.

From SDG&E's perspective, the key principle underlying the National Infrastructure Protection Plan is that there is a principal agency that has full-time responsibility to address cyber threats. This focus on protecting the national communications system (and other critical infrastructure) from attack, by providing the user-public with a single point of contact for reporting attacks and receiving information regarding emerging threats, will assure that the responsible authority will have the necessary resources, means and mission to prevent, mitigate or abate attacks now and in the future, with the support of those agencies with an interest in any given sector. Vesting the ultimate responsibility in a primary agency reduces the potential for confusing jurisdictional boundaries and priorities and distracting agencies from their more natural regulatory jurisdictions. In the context of attacks on the smart grid, as an example, SDG&E is concerned that this Commission and the FERC might be unclear as to which agency, despite their best intentions to cooperate in the detection and mitigation of the effects of these attacks, would presume to be the agency principally responsible for the federal response in any given situation where both the national broadband system and the interconnected power grid had both been targeted and disrupted. While both agencies might have an interest in the cybersecurity of the industries they regulate, neither has the resources capable of performing this role and neither has this role as a principal jurisdictional function under their enabling statutes. Under the umbrella of a larger, coordinated effort, SDG&E would expect that the respective and proper roles of these agencies can and will be harmonized and integrated effectively.

C. Summary

SDG&E appreciates this opportunity to address the Commission's ongoing consideration of cyber threats and the federal response to those threats. The Commission's efforts in identifying and addressing cybersecurity issues will affect the interests of the domestic energy industry and its consumers as that industry deploys and operates smart grid equipment,

applications and functionalities. Thus, if properly designed, the Commission's National Broadband Plan cybersecurity roadmap can protect the national interests in a smart, reliable power system as well as to the national communications system. SDG&E urges the Commission to place appropriate emphasis on capturing these benefits by reflecting, as it did in the National Broadband Plan, the emerging communications needs and priorities of the smart electricity grid as it continues its important work in the area of cybersecurity.

Respectfully submitted,

/s/ Alvin S. Pak

Alvin S. Pak
Senior Regulatory Counsel
San Diego Gas & Electric Company

Attorney for San Diego Gas & Electric Company
101 Ash Street, HQ12C
San Diego, California 92102
Telephone: 619.696.2190
Facsimile: 619.699.5027
Electronic Mail: Apak@SempraUtilities.com

September 23, 2010
San Diego, California